Communications of the Association for Information Systems

Volume 24 Article 34

6-1-2009

Current State of Information Security Research In IS

Humayun Zafar
The University of Texas at San Antonio, hzafar@kennesaw.edu

Jan Guynes Clark
The University of Texas at San Antonio

Communications of the Association for Information Systems

CAIS

Current State of Information Security Research In IS

Humayun Zafar

College of Business, The University of Texas at San Antonio

Humayun.Zafar@utsa.edu

Jan Guynes Clark

College of Business, The University of Texas at San Antonio

Abstract:

The importance of information security in a pervasive networked environment is undeniable, yet there is a lack of research in this area. In this study we conduct a comprehensive survey of the information security articles published in leading IS journals. We then compared the research themes with those of the IBM Information Security Capability Reference Model.

Keywords: information security, intrusion detection systems, computer crime, network security, privacy, spyware, computer viruses, security management, hacking, password protection, security models, information security

Volume 24, Article 34, pp. 557-596, June 2009

The manuscript was received 11/9/2007 and was with the authors 5 months for 2 revisions.

I. INTRODUCTION

Instances of systemwide breakdowns due to security breaches and their consequences have become fairly common, ranging from a halt in the online sales of World Series tickets [Slevin 2007], to research that shows a 2.1 percent decrease in market value within two days of a firm's announcement of a security breach [Cavusoglu et al. 2004a]. Although information security can have a great impact on organizations, IS research in this area is still in its infancy.

The term "information security" has many definitions. Depending upon one's viewpoint, it can be technical, behavioral, managerial, philosophical, and/or organizational. Von Solms [2006] characterizes information security in waves, progressing from technical to managerial to institutional and finally the information security governance wave. Greater emphasis on good corporate governance (which includes information security governance) and legal and regulatory requirements were described as the drivers behind the fourth wave. Following are a few definitions of information security:

- The process of protecting the availability, privacy, and integrity of information [Wise Geek]
- Proper use of data and controls to prohibit accidental or unauthorized use, destruction, or modification of information assets [Peltier 2001]
- The process of protecting the confidentiality, integrity and availability of information [Bishop 2003]
- "A well-informed sense of assurance that information risks and controls are in balance." [Anderson 2003. p. 310]

We prefer a more holistic view of information security, incorporating technology, processes, and people [Baskerville 1993; Straub and Welke 1998; Dhillon and Torkzadeh 2006; De Veiga and Eloff 2007]. As such, information security cannot be defined in one sentence. Following is our definition of the components of information security:

- Understanding the potential threats of an organization and assessing the risks associated with those threats
- Educating personnel in security awareness, code of conduct, and information security best practices
- Establishing policies and procedures to protect information assets from intentional or accidental misuse or loss
- Establishing policies and procedures to mitigate loss should security breaches occur
- Implementing and monitoring technologies to prevent or mitigate the loss from present or future security breaches
- Continuous assessment of technology, policies and procedures, and personnel to assure proper governance of information security issues
- Incorporating information security governance as an important part of corporate governance

Prior research on computer security has concentrated mostly on either identifying security as a socio-philosophical concern [Ratnasingham 1998], a socio-organizational concern [Dhillon and Backhouse 2001], or as a purely technical issue [Bass 2000; Wong et al. 2000; Li and Guo 2007; Yang and Huang 2007;]. Such delineation has possibly led to a situation where security is widely regarded as a field which lacks comprehensive research in IS [Paulson 2002; Kotulic and Clark 2004]. We contend that the information systems discipline can, and should, contribute to information security research.

The purpose of this research was to review information security research in leading IS journals, classify them according to the type of information security research conducted, and provide suggestions for further information security research by IS researchers. We therefore conducted a comprehensive review of information security research published in nine of the leading IS journals. We then classified the research according to the themes established by the IBM Information Security Capability Reference Model [IBM 2006]. For an article to be categorized as security, it had to have security or one of the IBM themes as a major construct and not as a side reference [For example see Alder et al. 2006]. In the following sections we present the journal selection process (Section II), discussion of the IBM Information Security Capability Reference Model (Section III), identification of current streams of research in security based on the IBM themes (Section IV), a summary of results (Section V), limitations of this study, and directions for future research (Section VI) .

Communications of the Association for Information Systems

II. SELECTION OF JOURNALS

Information Security research involves topics which are appropriate to the MIS discipline's core properties [Benbasat and Zmud 2003]. Since we are interested in what IS researchers are doing in regard to information security research, we focused only on IS discipline journals. Specifically, we reviewed journals that are a) highly ranked IS discipline journals [Peffers and Tang 2003]; b) promoted by the Association for Information Systems (AIS) Senior Scholars [Senior Scholars 2006]; and/or c) information security journals created primarily for the IS discipline.

IS Discipline Journals

For the purpose of this study, we referred to Peffers and Tang's [2003] top-50 IS ranked journals. We selected those journals ranked in the top 10 percent. Note that two journals tied for fifth place, resulting in six journals. Those journals include (**I&M* and *CAIS* tied for fifth place):

1. *MIS Quarterly (MISQ)*
2. *Information Systems Research (ISR)*
3. *Journal of Management Information Systems (JMIS)*
4. *European Journal of Information Systems (EJIS)*
5. *Information & Management (I & M)**
6. *Communications of the Association for Information Systems (CAIS)**

Senior Scholars Basket

In 2006, the IS Senior Scholars proposed that AIS adopt a basket of six journals which they deemed as "excellent" journals associated directly with the IS community [Senior Scholars, 2006].
That basket includes the following (in alphabetical order):

- European Journal of Information Systems (EJIS)
- Information Systems Journal (ISJ)
- Information Systems Research (ISR)
- Journal of the Association for Information Systems (JAIS)
- Journal of Management Information Systems (JMIS)
- MIS Quarterly (MISQ)

IS Discipline Security Journals

There are very few journals dedicated to information security research. The *Journal of Information Systems Security (JISSEC)* is a fairly new journal (first published in 2005). However, it is self-described as the "first IS Security journal" and "an official AIS SIGSEC publication" [JISSEC 2008]. SIGSEC is an AIS-sponsored security forum [http://ctans.okstate.edu/sigsec.htm]. Since *JISSEC* is, to our knowledge, the only security journal supported by an IS Special Interest Group, it was included in our sample of journals.

We agree that information security research is published in other journals, such as *Communications of the ACM, Computers & Security, and Management Science.* However, these journals are inter-disciplinary, not specifically targeted for the IS community. Although it is true that traditional ranking lists may not include research streams such as information security, the importance of concentrating on the leading journals in our field cannot be negated. Therefore, since our focus was information security research within the IS discipline, we only reviewed IS journals. Specifically, we reviewed the information security research that has been conducted, looking for trends in specific journals, or across time lines. We searched each of the journals from their first date of publication thru calendar year 2007. The journals in our sample, along with search range dates, are shown in Table 1.

III. CORE INFORMATION SECURITY THEMES

IBM Corporation has developed an Information Security Framework [IBM 2006] designed to provide an integrated, comprehensive view of an organization. The framework encompasses employee training, best practices, assessment tools, and an Information Security Capability Reference Model, based on the following core security "themes":

- Governance
- Privacy
- Threat Mitigation
- Transaction and Data Integrity
- Identity and Access Management
- Application Security
- Physical Security
- Personnel Security

Table 1. Journals Selected	
JOURNALS	**SEARCH RANGE**
CAIS	March, 1999 thru December, 2007
EJIS	January, 1993 thru December, 2007
I & M	March, 1977 thru December, 2007
ISJ	January, 1991 thru December, 2007
ISR	March, 1990 thru December ,2007
JAIS	March, 2000 thru December, 2007
JISSEC	March, 2005 thru December, 2007
JMIS	May, 1984 thru December, 2007
MISQ	March, 1977 thru December, 2007

The Information Security Capability Reference Model provides organizations with a baseline with which to assess their security posture. It is a comprehensive model that addresses technical, behavioral, and managerial issues related to information security. Thus, it supports our initial argument which calls for a more holistic approach toward information security. Although the model themes cover broad areas of information security, the assessment factors help to narrow down potential research areas associated with each theme. A description of the model and its components is shown in Table 2.

Table 2. IBM Information Security Capability Reference Model		
Security Theme	**Assessment**	
Governance	• Strategy and Information Security Policy • Security Compliance	• Security Risk Management • Governance Structure • Information Security Advisory
Privacy	• Policy, Practices and Controls • Privacy and Information Management Strategy	• Data, Rules, and Objects
Threat Mitigation	• Network Segmentation and Boundary Protection • Vulnerability Management	• Content Checking • Incident Management
Transaction and Data Integrity	• Business Process Transaction Security • Database Security	• Message Protection • Secure Storage • Systems Integrity
Identity and Access Management	• Identity Proofing • Access Control	• Identity Lifecycle Management
Application Security	• Systems Development Life Cycle	• Application Development Environment
Physical Security	• Site Management	• Physical Asset Management
Personnel Security	• Workforce Security	

Adapted from IBM [2006]

IV. STREAMS OF RESEARCH

One hundred and thirty-seven information security research articles were published in the basket of nine journals from their date of inception to December, 2007. We reviewed each of these articles and classified them according to IBM's Information Security Capability Reference Model. All but six research articles could be categorized into one of the eight themes. Each of those articles was related to the economics of information security. We therefore increased the number of information security themes to nine. A summary of the article classifications and the journals in which they appeared is shown in Table 3.

Table 3. Summary of Findings											
Journals/Themes	**MISQ**	**ISR**	**JMIS**	**EJIS**	**I&M**	**CAIS**	**JAIS**	**ISJ**	**JISSEC**	**Totals**	**Security %**
Governance	5	1	3	4	6	4	1	1	6	31	22.6
Privacy	1	5	1		5	5	2		3	22	16.1
Threat Mitigation			1		4	8	1		8	22	16.1
Transaction and Data Integrity	2	2	5	4	13	4	3		3	36	26.3
Identity and Access Management			1			3			1	5	3.7
Application Security					2			1	1	4	2.9
Physical Security					3					3	2.2
Personnel Security	1	1			2	1	2		1	8	5.8
Economics		2	1			1			2	6	4.4
Totals	9	11	12	8	35	26	9	2	25	137	
Journal %	6.6	8.0	8.8	5.8	25.5	18.9	6.6	2.9	18.5		100%

The majority of information security research appeared in I&M, CAIS, and JISSEC. We expected this. I&M is one of the older journals and covers a broad range of topics. While much newer, CAIS also covers a broad range of topics, but also publishes significantly more articles each year. Finally, JISSEC is the newest of the journals, but dedicated to information security research. As shown, more than 80 percent of the information security research published in our basket of leading IS journals is in the following themes: Transaction and Data Integrity (26 percent), Governance (23 percent), Threat Mitigation (16 percent), and Privacy (16 percent).

To ascertain if there is a link between the years of publication and the security themes, we separated each publication by decades. Tables 4 thru 7 display the research published during the 1970s, 1980s, 1990s, and 2000s (up to and including 2007). We were not surprised to see that very few information security research papers were published in the 1970s (Table 4). Of our journal basket, only MISQ and I&M were in print during the 1970s. And, of those journals, only I&M published any information security research. During the 1970s, only two of the nine themes were researched in leading IS journals: Privacy and Transaction and Data Integrity.

Table 4. Information Security Research in the 1970s		
Journals/Themes	I&M	Totals
Governance		
Privacy		1
Threat Mitigation		
Transaction and Data Integrity		2
Identity and Access Management		
Application Security		
Physical Security		
Personnel Security		
Economics		
Totals		3

During the 1980s, we saw a substantial increase in the number of information security research articles and the themes researched. During this time period, information security articles appeared in *I&M*, *JMIS*, and *MISQ*; five of the nine themes were represented (Table 5). As shown, Transaction and Data Integrity was the primary area of IS security research, and at least one article in that area appeared in the journals that published information security research during that time period.

Communications of the Association for Information Systems

Table 5. Security in the 1980s				
Journals/Themes	MISQ	JMIS	I&M	Totals
Governance	1		1	2
Privacy			2	2
Threat Mitigation				
Transaction and Data Integrity	1	1	5	7
Identity and Access Management				
Application Security			1	1
Physical Security			2	2
Personnel Security				
Economics				
Totals	2	1	11	14

Although there was little change in the number of security publications in the 1980s versus those in the 1990's (Table 6), seven of the nine research themes were represented, indicating a broader range of information security research. More than 50 percent of the information security research was focused on Governance and Privacy. Also note that information security research appeared in six of our basket of nine journals.

Table 6. Security in the 1990s								
Journals/Themes	MISQ	ISR	JMIS	EJIS	I&M	CAIS	ISJ	Totals
Governance	3	1	1	1	1			7
Privacy					1			1
Threat Mitigation					3			3
Transaction and Data Integrity					3			3
Identity and Access Management			1					1
Application Security					1			1
Physical Security					1			1
Personnel Security	1	1			1			3
Economics								
Totals	4	2	2	1	11			20

As shown in Table 7, we have experienced a significant increase in the amount of information security research since 2000. During this decade, 100 security research articles have appeared in the basket of nine journals. This is a 500 percent increase in the number of information security articles published in the 1990s. Since 2000, all themes except Physical Security were represented. Note that Economics of IS security first appeared as a research stream in this decade.

Table 7. Security in the 2000s										
Journals/Themes	MISQ	ISR	JMIS	EJIS	I&M	CAIS	ISJ	JAIS	JISSEC	Totals
Governance	2		1	3	4	4	1	1	6	22
Privacy	1	5	1		1	5		2	3	18
Threat Mitigation			1		1	8		1	8	19
Transaction and Data Integrity	1	2	4	4	3	4		3	3	24
Identity and Access Management						3			1	4
Application Security							1		1	2
Physical Security										0
Personnel Security					1	1		1	2	5
Economics		2	1			1			2	6
Totals	4	9	8	7	10	26	2	8	26	100

Following is a brief overview of each of the articles, presented in chronological order, and classified according to theme and method of assessment.

Governance

Governance involves the development of strategic and compliance programs which result in a robust management framework. Leadership and effective policies and procedures are important characteristics for well-governed organizations. Organizations must assure the critical assets are identified and protected against possible risks. Following is a brief discussion of how governance, as applied to information security, has been addressed in our basket of nine journals:

Strategy and Information Security Policy

This includes any policies pertaining to information security and their overall effect on the organization.

- Hammer [1988] cited situations in which lack of information security policy and procedure can result in loss or inefficient access to data.
- Straub and Nance [1990] proposed policies and managerial involvement in the detection and discipline of computer abuse within an organization.
- Straub [1990a] applied General Deterrence Theory to determine if management's investment in security was a deterrent to computer abuse.
- Wang [1994] surveyed IS managers in the Republic of China and cited security and control as a major issue.
- Baskerville [2005] discussed the need for balancing both business and information warfare paradigm views to improve information security management.
- Morin and Pawlak [2006] presented a framework for corporate policy management based on Digital Rights and Policy Management (DRM).
- Backhouse et al. [2006b] applied the Circuits of Power theoretical framework to BS7799, a British Standard which later became ISO 17799, an International Standard for information security management.
- Fjermestad et al. [2006] addressed the usage of mobile communication technologies from three perspectives: service providers, organizations, and users of mobile cellular services.
- Siponen and Iivari [2006] advanced six design theories (liberal-intuitive, prima-facie, virtue, utilitarian, conservative-deontological, and universalizability) by using their principles to guide the development of IS security policies.

Security Compliance

Security compliance includes understanding, implementing and maintaining regulatory compliance, controls, audit and response systems, and standards related to information security.

- Lockman and Minsky [1989] introduced the need for internal controls for large scale financial information systems.
- Post and Kagan [2000] reviewed the advantages and disadvantages of restrictive versus proactive security policies designed to prevent virus outbreaks.
- Kotulic and Clark [2004] discussed how their attempt to study security compliance failed because of the sensitive nature of the topic.
- Siponen [2005] reviewed traditional IS security (ISS) approaches and compared their underlying key assumptions.
- Ma and Pearson [2005] empirically validated the ISO 17999 international security management standard.

- Shao et al. [2005] used a case-study approach to demonstrate a model for online dispute resolution by maintaining a chain of evidence.
- Goel et al. [2006] discussed the procedures involved in security audit.

Security Risk Management

Security Risk Management includes threat risk assessments, profiling of assets, project risk management, and security risk management.

- Loch et al. [1992] surveyed senior MIS managers to determine security threats and, of those, which were the most serious.
- Straub and Welke [1998] provided guidelines for how managers can be better aware of information security controls available to them so that they can reduce the impact of damage or loss.
- Biros et al. [2002] conducted a field study to devise methods of improving deception detection.
- Willison and Backhouse [2006] extended a model of system risk based on the perspective of the offender.
- Goodman and Ramer [2007] discussed the information security risks associated with global sourcing of IT services and provided suggestions for mitigating these risks.
- Choobineh et al. [2007] provided the results of a panel discussion on management of information security, formerly presented at the 2007 AMCIS conference.

Governance Structure

Governance Structure is based on defining the goals and objectives of information security management and establishing overseeing bodies and structures of responsibility which monitor and govern all aspects of an organization's information security.

- Lewis et al. [1995] operationalized the information resource management (IRM) construct based on the following dimensions: Chief Information Officer, Planning, Security, Technology Integration, Advisory Committees, Enterprise Model, Information Integration, and Data Administration.
- Backhouse and Dhillon [1996] provided a conceptual framework for improving information systems security by analyzing the structures of responsibility.
- Lewis and Byrd [2003] operationalized the Information Technology Infrastructure (ITI) concept by identifying seven dimensions: Chief Information Officer, IT Planning, IT Security, Technology Integration, Advisory Committee, Enterprise Model, and Data Administration.
- von Solms et al. [2005] developed a framework for evaluating information security.
- Dhillon and Torkzadeh [2006] interviewed managers, using a value-focused approach, to identify the objectives of IS security.
- Sun et al. [2006] developed a methodology for risk analysis of information systems security (ISS) using the Dempster-Shafer theory of belief functions.
- Carlsson and Jacobson [2006] presented a security consistency model that describes a systemic view of information networks and their risk environment.
- McFadzean et al. [2006] surveyed the literature on information security and security governance and provided suggestions for further research.
- Sridhar and Ahuja [2007] presented a case study of a business school in India that implemented a security management infrastructure.

Privacy

In this study, information privacy is relegated to the area of using privileged information with malicious intent. References to privacy as solely being a right of an individual [e.g. Straub 1990b] were not included.

Policy, Practices, and Controls

This includes development of taxonomies, as well as rules definitions, impact assessments, and awareness and training.

- Turn [1978] presented an overview of issues in privacy protection related to record-keeping systems.
- Greenaway and Chan [2005] reviewed the information privacy literature and suggest applying the Resource Based View (RBV) of the firm and Institutional Theory to explain an organization's behavior toward information privacy.
- Hann et al. [2007] applied the expectancy-based theory of motivation to analyze strategies to mitigate on-line consumer concerns for information privacy.

Privacy and Information Management Strategy

This assessment includes description of a privacy information strategy, requirements and compliance processes, as well as any incident response situations.

- Cattela [1981] discussed how information is a corporate asset, and that a clear distinction should be made between neutral (e.g. name, department, etc.) and sensitive (e.g. personnel file, salary, etc.) data.
- Kim et al. [2002] studied how trust-assuring statements on web-based stores impact consumer trust.
- Faja and Trimi [2003] studied customer perceptions concerning privacy of personal information and its relation to the growth of on-line businesses.
- Malhotra et al. [2004] studied the lack of consumer confidence in information privacy and its direct impact on the growth of e-commerce.
- Speikermann and Ziekow [2005] provided suggestions for designing "privacy friendly" RFID technologies to alleviate consumer fears.
- Ahluwalia and Varshney [2005] proposed methods of improving quality of service of mobile commerce transactions.
- Van Slyke et al. [2006] surveyed consumers to determine their concerns for information privacy and their readiness to transact with well-known versus less-well-known Web merchants.
- Shim et al. [2006] investigated the increasing use of RFID in cell phones and how the ability of tracking raises questions about an individual concerns for privacy.
- Shim et al. [2007] discussed privacy and security concerns such as the ability to keep personal affairs private while using wireless technology.
- Park et al. [2007] studied how e-mail users respond to spam and how it affects their concerns for information privacy.
- Hui et al. [2007] conducted an exploratory field study to assess the value of privacy statements and privacy seals on Internet sites.

Data, Rules, and Objects

This includes development of classification and/or business process models.

- Roos [1981] stressed the need for control of confidentiality of information by both the system and end users.

- Frank et al. [1991] investigated the problems of monitoring behavior of personal computer users in organizations.
- Ariss [2002] recommended ways in which electronic monitoring of employees can be conducted while addressing concerns for privacy.
- Ives and Krotov [2006] discussed a case in which AOL's public release of user search information caused a debate over privacy.
- Li and Sarkar [2006] proposed a perturbation method for categorical data which organizations can use to prevent or limit disclosure of sensitive data.
- Dinev and Hart [2006] proposed a calculus based model to explain the tradeoff between E-commerce privacy and outcomes that are perceived to be worth the risk of information disclosure.
- Garfinkel et al. [2007] developed a method to allow the release of individual data while providing confidentiality protection to the data subjects.
- Dhillon and Chapman [2006] presented the case of Doubleclick and their potential privacy violations.

Threat Mitigation

Threat mitigation is concerned with network segmentation (e.g. network security infrastructure, intrusion detection, and remote access), vulnerability management (e.g. scanning, patching, and standard operating procedures), content checking (e.g. data filtering and virus protection) and incident management issues (e.g. forensics and event correlation). Should a security breach occur, threat mitigation entails lessening the severity of the breach.

Network Segmentation and Boundary Protection

Network boundaries are becoming more and more ethereal, no longer limited to a single organization. Organizations continue to provide consumers and suppliers greater access to their networks. However, they must be aware of the increased risk of perpetrators also accessing their networks. This section includes development of intrusion defense mechanisms, boundary security, remote access, and network security infrastructures.

- Stephens and Snyder [1991] developed a customized "gateway" solution which meets the criteria of security for the exchange of data between dispersed units of a business.
- Ryan and Bordoloi [1997] surveyed technical IS professionals to evaluate their concerns for security threats in distributed systems.
- Boncella [2004] provided a theoretical foundation for understanding the needs and techniques of Web Services (WS).
- Shanley and Premkumar [2005] developed and tested a wireless intrusion detection system to detect man-in-the-middle attacks.
- Reed [2005] provided a tutorial on the administration of remote servers and network architecture.
- Halonen [2006] provided a case study of how user authentication was established in an interorganizational system of users from multiple universities.
- Cazier and Medlin [2006] reviewed passwords created by end-users on an e-commerce site and estimated their crack times.
- Korzyk et al. [2006] developed a conceptual model of an integrated information security management system (ISMS).
- Ye et al. [2007] developed and tested an intrusion detection system based on packets of varying sizes.

- Yeh and Chang [2007] conducted a cross-industry study of IS managers' perceptions of information security threats and countermeasures.

Vulnerability Management

Vulnerability Management includes assessment of any vulnerabilities a system may have, along with any patches which may be needed in the standard operating environment.

- Joseph and Blanton [1992] identified the organizational and technical aspects of a total infector control program which can be used to appraise infector threats and risks within an organization.
- Knapp et al. [2003] proposed an innovative framework which brackets the defense mechanisms of cellular biology with the security processes of networked systems which defend against attacks.
- Panko [2003] described the damage caused by the Slammer worm and stressed the importance of patch management.
- Siponen et al. [2006] employed meta-notation approach to develop a secure information system (SIS) framework that defines requirements for SIS design methods.

Content Checking

Worms, viruses, and spyware are becoming increasingly sophisticated. Instead of attacking a relatively few systems, some malware can attack virtually any system connected to the Internet. This section includes elements related to virus protection and content filtering to prevent spam and phishing.

- Goel et al. [2005] presented a case in which a botnet was used to attack an organization and provided suggestions for protecting the network infrastructure.
- Schryen [2007] evaluated the effectiveness of current anti-spam measures and suggested other ways of decreasing the volume of spam.
- Yue and Cakanyildirim [2007] proposed an analytical model which studies the decisions involved in the intrusion prevention process.
- Bose and Leung [2007] provided a tutorial on phishing and offered suggestions for detecting and/or preventing it.

Incident Management

Incident Management deals with forensics, event correlations, and procedures to manage a security breach should it occur

- Bagchi and Udo [2003] used a sparse data set to identify growth characteristics of computer and internet related crimes.
- Stafford and Urbaczewski [2004] discussed the legitimate and non-legitimate roles of spyware and provided ways in which to protect against spyware.
- Lim [2006] described a model for developing a computer forensics course.
- Ray et al. [2007] presented a forensic path verification technique to monitor and identify false Internet pathways.

Transaction and Data Integrity

Transaction and Data Integrity is concerned with business process transaction security (e.g. fraud detection and transaction security), database security (e.g. configuration and control), message protection (e.g. encryption and message security), secure storage (e.g. data storage, archiving, retrieval, and destruction), and systems integrity (e.g. secure systems management and business continuity planning).

Business Process Transaction Security

This includes detection of fraudulent activities, as well as maintenance of data transactions.

- Lucas [1985] presented a review of the Social Security Administration's information processing efforts and potential fraud by the US General Accounting Office.
- Tan and Teo [2000] surveyed consumers to determine the factors that influence their decision to adopt Internet banking.
- Bajaj [2000] interviewed senior IS managers to determine the factors that influence their decision to adopt new computing architectures.
- Rangnathan and Ganapathy [2002] surveyed online shoppers to determine the characteristics of a business-to-consumer (B2C) Web site that make it effective.
- Lee [2003] surveyed Internet-based information systems managers in Korea to determine issues and problem related to developing an Internet-based system.
- Kim et al. [2004b] surveyed potential and repeat e-commerce customers to determine their differences in trust.
- Soliman and Janz [2004] surveyed IS and logistics managers and identified critical factors in their decision to adopt Internet-Based Interorganizational Information Systems (IBIS).
- Ba et al. [2005] used the evolutionary game theory approach to analyze conventional and electronic markets, with emphasis on security and product quality uncertainty.
- Fang et al. [2005] proposed a conceptual model for wireless device adoption based perceived usefulness, perceived ease of use, perceived playfulness, and perceived security.
- Looi [2005] proposed a research model for e-commerce adoption which considers five factors: relative advantage, IT knowledge, competitive pressure, government support, and security.
- Molla et al. [2006] presented a case study and discussed why an e-commerce business failed.
- Kim and Benbasat [2006] studied the impact of trust-assuring arguments in obtaining consumer trust in Internet stores.
- Verhagen et al. [2006] studied the relation between consumer perception of risk and trust and the attitude toward purchasing at an electronic marketplace (EM).
- Pavlou et al. [2007] studied the business-to-consumer e-commerce paradigm, and which factors play the role of inhibitors in its adoption.

Database Security

This section explores configurations of a database along with any master data controls which may be needed in an organization.

- Bussolati and Martella [1981] presented a multi-level logical security architecture for managing distributed data
- Egyhazy [1985] addressed the issue of database machine technology and architecture in embedded computer systems.
- Croker [1987] proposed several methods of reducing database transaction lock time.

- Adam and Jones [1989] presented a security control method that decreases the probability of compromising a statistical database.
- Sarathy and Muralidhar [2002] simulated a model for protecting confidential numerical data in organizational databases.
- Asif and Mandviwalla [2005] analyzed the technical and business issues associated with the adoption of RFID in organizations.
- Avourdiadis et al. [2005] presented an extensible database architecture for unifying data from multiple databases.

Message Protection

This includes usage of key and encryption algorithms to protect messages.

- Hammer [1977] predicted that with advances in chip technologies, data security would be provided through cryptographic hardware.
- Murray [1979] provided methods for decreasing storage requirements of encrypted data.
- Varshney [2003] examined the current state of mobile systems and discussed the challenges associates with their wide-scale deployment.
- Gupta et al. [2004] explored the use of digital signatures in obtaining secure electronic transactions.
- Peffers et al. [2007] provided an example of how the design science approach could be used to enhance voice and video over IP standards.

Secure Storage

This section pertains to secure methods of data retrieval, data storage protection, data destruction, and archiving.

- Thuraisingham [1993] discussed the need for, and security issues related to, a multilevel secure data model for information retrieval.
- Thuraisingham [1995] proposed and presented an example of a multi-level secure information retrieval system.
- Perlman [2005] proposed of method of making data readily available when needed, yet destructed when it reaches a given expiration time.

Systems Integrity

This section includes development of systems and controls which provide for information security and continuity of the business.

- Tam [1989] proposed a secure model for online securities trading.
- Boockholdt [1989] identified methods in which a personal computer (PC) needs to achieve security on a network and any subsequent threats that may be caused by the PC itself.
- Adams and Chang [1993] proposed a keypad interface system to maximize security and use.
- Currie and Seltsikas [2001] explored the supply-side of IT outsourcing and discussed the associated risks.
- Yang et al. [2004] developed a framework which addresses the myths and beliefs associated with wireless communication.
- Muntermann and Heiko [2006] proposed a secure information and transaction processing infrastructure for mobile brokerage services.

Identity and Access Management

Identity and access management includes identity proofing through background screening and alternative methods of credential management. Its focus is on identifying users, protecting confidential information from unauthorized users, providing authorized users, and secure, controlled access to resources.

Identity Proofing

This includes methods which can be used to have access management, and establishment of identities through various security protocols such as usernames and passwords.

- Zviran and Haga [1999] studied the characteristics of user-selected passwords such as number of characters, frequency of changing passwords, and method of choosing passwords.
- Boukhonine et al. [2005] provided a tutorial on how biometric technologies can be used to improve security.

Access Control

Access control assesses ways in which authentication mechanisms can be implemented, and how a single sign-on can be established to counter a hacker's activities.

- Bento and Bento [2006] empirically tested a hacking model based on attacks and hacker behavior.
- Zviran and Erlich [2006] compared a variety of authentication mechanisms and discussed the problems associated with each of them.
- Beebe and Clark [2007] created a discriminant model for predicting hacker behavior.

Application Security

An Application Security assessment entails code review, secure coding practices, and secure policies and procedures to manage the Systems Development Life cycle (SDLC). It is generally far less costly to prevent a security error, rather than to fix it once it occurs.

Systems Development Life Cycle (SDLC)

This section includes procedures which can be used to ensure security throughout the systems development lifecycle process.

- Sumner [1986] evaluated approaches to systems development based on various characteristics of the application.
- Im and Epps [1992] studied a trend of unauthorized software copying by faculty, staff, and students of a university.
- Tryfonas [2007] applied organizational metaphors to discuss the practice of developing secure information systems.

Application Development Environment

This assesses how secure coding practices, better design patterns, and an operational application support environment can assist in development of secure applications.

- Payne [2002] presented arguments, both in favor and against, open source software and analyzed those arguments in relation to empirical evidence of system security.

Physical Security

Security is not an issue which can exclusively be handled with software. There is a requirement for physical barriers as well. Physical Security describes the measures taken to protect facilities, resources, and information from potential attackers.

Site Management

This includes protocols such as site planning and management which will ensure in security of assets in the event of a catastrophe, for example, fire, earthquakes, et cetera.

- Duffy [1980] provided a case study of physical hazard (fire) and subsequent recovery operations in a computer room.

Physical Asset Management

Physical asset management explores actual asset and document management which may be helpful in guarding against security threats.

- Boockholdt [1987] assessed the impact of microcomputers on system integrity, and proposed measures to safeguard against security threats.

- Koh and Watson [1998] investigated the relationship between data security, ownership, and standards.

Personnel Security

Personnel security relates to the workforce of an organization. Assessment factors include awareness training, code of conduct, and employment lifecycle management. The issue of ethics in security varies from behavioral research to building a network infrastructure.

Workforce Security

Personnel play a very important role in establishing and maintaining information security within an organization. Unless properly trained and educated in the use of technology, security awareness and organizational code of conduct, they can inadvertently introduce threats to the organizations, its suppliers, and/or its consumers.

- Goodhue and Straub [1991] surveyed computer users to determine their level of computer security concerns.

- Harrington [1996] surveyed IS employees to determine ethical judgments and intentions regarding a variety of computer abuses.

- Gattiker and Kelley[1999] applied the "domain of morality" approach to gauge how users felt about certain computer related behaviors such as loading a computer virus on a network.

- Whitworth and Zaic [2003] developed the Web of Systems Performance (WOSP) framework for modeling advanced network structures such as the Internet.

- Alder et al. [2006] conducted a field study to determine the impact on trust if employees are given advance notice that their computer use is monitored.

- Angell [2007] questioned of role of ethics and morality in information security.

- Dinev and Hu [2007] extended the theory of planned behavior to study attitudes toward protective technologies such as firewalls and anti-virus software.

- D'Arcy and Hovav [2007] surveyed computer users to determine how effective security policies, education, training and awareness programs, and computer monitoring were in deterring computer abuse.

Information Security Economics

Applying economic theory to information security research is relatively new. We found six articles related to economics and security within our basket of nine journals. While this is a relatively small number of articles, note that there were no publications related to this topic prior to 2004.

Information Security Investment

Decision-making based on investment in information security is a difficult process. Normally, one would analyze return on investment to determine whether to invest. However, in most information security technologies, it is better to assess potential loss if one does not invest.

- Cavusoglu et al. [2004b] discussed four elements that IT managers should consider when managing the security function: estimation of breach costs, risk management, cost-effective configuration of technology, and value from deployment of multiple security technologies.

- Ramachandran and White [2005] developed a methodology for assessing the impact of IT investment in security tools and products.

- Gal-Or and Ghose [2005] developed an analytical framework (using Game Theory) to describe the competitive implications of sharing information related to security and investments in security technologies.

- Cavusoglu et al. [2005] discuss four economic perspective elements that information security managers need to be concerned about: estimated cost of a security breach, risk management, cost effective configuration, and value from deployment of multiple technologies

- Backhouse et al. [2006a] proposed a market-oriented solution to solving the problem of digital certificate lemons.

Consumer Choice

Consumer choice integrates privacy concerns of an individual with what is available in terms of enhancing the security of online transactions using an economics lens.

- Chellappa and Shivendu [2007] developed an economic model for on-line privacy, comparing profits, consumer surplus, and social welfare among privacy versus convenience seekers

IV. SUMMARY OF INFORMATION SECURITY RESEARCH AND SUGGESTIONS FOR FURTHER RESEARCH

Table 8 provides a summary of the information security research conducted in our basket of nine journals since their date of inception. We also included a brief description of the research methods, theories, and level of analysis for each theme. The table shows how varied information security research in IS is and how it has the potential to be advanced further.

Directions for Future Research

Note that each of the themes presented in the IBM Information Security Capability Reference Model were represented, and all but two assessment areas for these themes are represented. Specifically, under the Governance theme, there is no research regarding the Information Security Advisory team. The other assessment area which lacked research was the Application Development Environment, part of the Application Security Theme. Although each of the themes are addressed in the IS literature, there remains a dearth of information security in these journals. We suggest that future researchers review the themes, their associated assessments, and existing research in the area to determine directions for future research. For example, we found no research in Governance and Information Security Advisory Team Assessment. Following are a few examples of potential research questions to study in this area:

- What are the potential pitfalls of a consultant conducting a security risk analysis?

- What are the potential pitfalls of a consultant developing an organization's governance structure?

- What are the desired qualifications of an information security consultant?

- What are the legal issues associated with an information security consultant's breach of security?

We also predict growing emphasis in the areas of information security economics (e.g. Campbell et al. [2003]), information sharing (e.g. Sharpe [2003]) and threat mitigation, particularly in regard to network segmentation and boundary protection (e.g. Han and Cho [2006]; Jain et al. [2006]; Verdon [2006]; Ballard and Lopresti [2007]; Roberts [2007]; Rodwell et al. [2007]). The need for an actual experiment is highly evident in this area since it is the only true method of determining causal relations (Shadish et al. [2002]). These studies also show how security research is dominated by the technical nature of the subject, hence presenting the need for a more holistic approach towards advancing in this area. However, most firms have no incentive for making security breaches public, so current research is limited. This discrepancy could potentially be glaring, and therefore needs to be explored further.

Table 8. Information Security Themes Researched in IS Journals				
Security Themes	**Level of Analysis**	**Theories**	**Methods Used**	**Assessments**
Governance	Individual, Business, Organization, Marketplace	Circuits of power, adoption theories, liberal-intuitive, prima-facie, virtue, utilitarian, conservative-deontological, universalizability, and Dempster-Shafer	Survey, interviews	Strategy and Information Security Policy, Security Compliance, Security Risk Management, Governance Structure
Privacy	Individual, Group, Business, Organization	Client/Server, organization theory, strategic management, calculus, risk management, design theory, Theory of Planned Behavior (TPB), institutional, resource based view, expectancy, motivation, calculus, and linear programming	Simulation, tutorials, SEM, models	Privacy and Information Management Strategy, Policy, Practices and Controls, Data, Rules and Objects
Threat Mitigation	Individual, Business, Organization	Cellular biology, network programming, client/server, diffusion of innovation, dispute resolution, systems development, and secure information systems	Survey, experiments, evidence management, chain of evidence	Network Segmentation and Boundary Protection, Vulnerability Management, Content Checking, Incident Management
Transaction and Data Integrity	Individual, System, Business, Organization	Encryption, decryption, public/private key, supply and demand, diffusion of innovation, game theory, Technology Acceptance Model (TAM), social context, database management, statistics, linear models, and logical architecture	Simulation, survey, trust models, interviews	Business Process Transaction Security, Database Security, Message Protection, Secure Storage, Systems Integrity
Identity and Access Management	Individual	Behavioral theories	Model	Identity Proofing, Access Control, Identity Lifecycle Management
Application Security	Business	Micro-computing, and software development lifecycle	Simulation, survey	Systems Development Life Cycle
Physical Security	Business, Organization	Morale	Survey	Site Management, Physical Asset Management
Personnel Security	Individual	Morality, socio-economic theory, Web of Systems Performance, and TPB	Survey	Workforce Security
Information Security Economics	Individual, Organization, Industry, Marketplace	Game theory, cost benefit analysis, and risk management	Survey, interviews	Information Security Investment, Consumer Choice

V. SUMMARY AND CONCLUSIONS

We conducted a comprehensive survey of all prior information security research published in *MISQ, ISR, JMIS, EJIS, CAIS, I&M, JAIS, JISSEC,* and *ISJ* from their date of inception. This is the first known study of this type. We identified nine themes of security, based on eight themes in IBM's Information Security Capability Reference Model and added information security economics. This is a relatively new area of information security research, and we feel strongly that it should not be omitted.

Limitations

It may be argued that a comprehensive survey of security articles in only nine journals may not give a clear indication about the status of IS research on security. This is true to some extent, but our focus was on information

security research conducted by IS researchers, and most likely to be read by IS researchers and professionals. Therefore, we focused on leading IS journals.

We also recognize that the categorization of studies into certain themes may not have been independent. For example, a study on privacy may also deal with access control. Therefore, there is some subjective assignment. This is mitigated to some extent through a more careful analysis of the research in question.

ACKNOWLEDGMENTS

We would like to acknowledge Dr. Joey F. George, Ms. Terri Davis, and the anonymous reviewers for their valuable input during the review process.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the paper on the Web, can gain direct access to these linked references. Readers are warned, however, that:
1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Adams, D. A. and S. Y. Chang. (1993). "An Investigation of Keypad Interface Security," *Information & Management* (24), pp. 53-59.

Adam N. and D. H. Jones. (1989). "Security of Statistical Databases with an Output Perturbation Technique," *Journal of Management Information Systems* (6)1, pp. 101-110.

Ahluwalia, P. and U. Varshney. (2005). "Supporting Quality-of-Service of Mobile Commerce Transactions," *Communications of the Association for Information Systems* (16), pp. 421-434.

Alder, G. S., T. W. Noel, and M. L. Ambrose. (2006). "Clarifying the Effects of Internet Monitoring on Job Attitudes: The Mediating Role of Employee Trust," *Information & Management* (43), pp. 894-903.

Anderson, J. M. (2003). "Why We Need a New Definition of Information Security," *Computers & Security* (22)4, pp. 308-313.

Angell, I. (2007). "Ethics and Morality: A Business Opportunity for the Amoral?", *Journal of Information System Security* (3)1, pp. 3-18.

Ariss, S. S. (2002) "Computer Monitoring: Benefits and Pitfalls Facing Management" *Information & Management* (39), pp. 553-558.

Asif, Z. and M. Mandviwalla. (2005). "Integrating the Supply Chain with RFID: A Technical and Business Analysis," *Communications of the Association for Information Systems* (15), pp. 393-427.

Avourdiadis, N., A. Blyth, and P. Thomas. (2005). "SoapSY: Unifying Security Data from Various Heterogeneous Distributed Systems into a Single Database Architecture," *Journal of Information System Security* (1)2, pp. 26-52.

Ba, S. et al. (2005). "Choice of Transaction Channels: The Effects of Product Characteristics on Market Evolution," *Journal of Management Information Systems* (21)4, pp. 173-197.

Backhouse, J., J. Baptista, and C. Hsu. (2006a). "Rating Certificate Authorities: A Market Approach to the Lemons Problem," *Journal of Information System Security* (2)2, pp. 3-14.

Backhouse, J. and G. Dhillon. (1996). "Structures of Responsibility and Security of Information Systems," *European Journal of Information Systems* (5), pp. 2-9.

Backhouse, J., C. W. Hsu, and L. Silva. (2006b). "Circuits of Power in Creating De Jure Standards: Shaping an International Information Systems Security Standard," *Management Information Systems Quarterly* (30), pp. 413-438.

Bagchi, K. and G. Udo. (2003). "An Analysis of the Growth of Computer and Internet Security Breaches," *Communications of the Association for Information Systems* (12), pp. 684-700.

Bajaj, A. (2000). "A Study of Senior Information Systems Managers' Decision Models in Adopting New Computer Architecture," *Journal of the Association for Information Systems* (1) Paper 4, pp. 1-55.

Ballard, L., and D. Lopresti. (2007). "Forgery Quality and Its Implications for Behavioral Biometric Security," *IEEE Transactions on Systems, Man, and Cybernetics Part B: Cybernetics*. (37)5, pp. 1107-1118.

Baskerville, R. (1993). "Information Systems Security Design Methods: Implications for Information Systems Development," *ACM Computing Surveys* (25), pp. 375-414.

Baskerville, R. (2005). "Information Warfare: A Comparative Framework for Business Information Security," *Journal of Information System Security* (1)1, pp. 23-50.

Bass, T. (2000). "Intrusion Detection Systems and Multisensor Data Fusion," *Communications of the ACM* (43)2, pp. 99-105.

Beebe, N. L. and J. G. Clark. (2007). "A Model for Predicting Hacker Behavior," *Journal of Information System Security* (3) 3, pp. 3-20.

Belanger, F., J. S Hiller, and W. J. Smith. (2004). "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes," *The Journal of Strategic Information Systems* (11)3-4, pp.245-270.

Benbasat, I. and R. W. Zmud. (2003). "The Identity Crisis Within the IS Discipline: Defining and Communicating the Discipline's Core Properties," *Management Information Systems Quarterly* (27)2, pp. 183-194.

Bento, A. and R. Bento. (2004). "Empirical Test of a Hacking Model: An Exploratory Study," *Communications of the Association for Information Systems* (14), pp. 678-690.

Biros, D., J. F. George, and R. W. Zmud. (2002). "Inducing Sensitivity to Deception in Order to Improve Decision Making Performance: A Field Study," *Management Information Systems Quarterly* (26)2, pp. 119-144.

Bishop, M. (2003) .*Computer Security, Art and Science.* Addison-Wesley, Boston, MA.

Boncella, R. (2004). "Web Services and Web Services Security," *Communications of the Association for Information Systems* (14), pp. 344-363.

Boockholdt J. L. (1987). "Security and Integrity Controls for Microcomputers: A Summary Analysis," *Information & Management* (13), pp. 33-41.

Boockholdt, J. L. (1989). "Implementing Security and Integrity in Micro-Mainframe Networks," *Management Information Systems Quarterly* (13)2, pp. 134-144.

Bose, I. and A. C. M. Leung. (2007). "Unveiling the Mask of Phishing: Threats, Preventive Measures, and Responsibilities," *Communications of the Association for Information Systems* (19), pp. 1-39.

Boukhonine, S., V. Krotov, and B. Rupert. (2005). "Future Security Approaches and Biometrics," *Communications of the Association for Information Systems* (16), pp. 937-966.

Bussolati U. and G. Martella. (1981). "Treating Data Privacy in Distributed Systems," *Information & Management* (4), pp. 305-315.

Campbell, K. et al. (2003). "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," *Journal of Computer Security* (11)3, pp. 431-448.

Carlsson, B. and A. Jacobsson. (2006). "Security Consistency in Information Ecosystems: Structuring the Risk Environment on the Internet," *Journal of Information System Security* (2)1, pp. 3-26.

Cattela, R. C. (1981)."Information as a Corporate Asset," *Information & Management* (4), pp. 29-37.

Cavusoglu, H., M. Birendra, and S. Raghunathan. (2004a). "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers," *International Journal of Electronic Commerce* (9)1, pp. 69-104.

Cavusoglu, H., M. Birendra, and S. Raghunathan. (2005). "The Value of Intrusion Detection Systems in Information Technology Security Architecture," *Information Systems Research* (16)1, pp. 28-46.

Cavusoglu, H., H. Cavusoglu, and S. Raghunathan. (2004b). "Economics of IT Security Management: Four Improvements to Current Security Practices," *Communications of the Association for Information Systems* (14), pp. 65-75.

Cazier, J. and B. D. Medlin. (2006). "How Secure Is Your Password? An Analysis of E-Commerce Passwords and Their Crack Times," *Journal of Information System Security* (2)3, pp. 69-82.

Chellappa, R. K. and S. Shivendu. (2007). "An Economic Model of Privacy: A Property Rights Approach to Regulatory Choices for Online Personalization," *Journal of Management Information Systems* (24)3, pp. 193-225.

Choobineh, J., G. Dhillon, M. R. Grimaila, and J. Rees. (2007). "Management of Information Security: Challenges and Research Directions," *Communications of the Association for Information Systems* (20) pp. 958-971.

Christie, B. (1981). *Face to File Communication: A Psychological Approach to Information Systems*. New York: Wiley.

Croker, A. (1987). "Improvements in Database Concurrency Control with Locking," *Journal of Management Information Systems* (4)2, pp. 74-92.

Currie, W. and P. Seltsikas. (2001). "Exploring the Supply-Side of IT Outsourcing: Evaluating the Emerging Role of Application Service Providers," *European Journal of Information Systems* (10), pp. 123-134.

D'Arcy, J. and A. Hovav. (2007). "Towards a Best Fit Between Organizational Security Countermeasures and Information Systems Misuse Behaviors," *Journal of Information System Security* (3)2, pp. 3-30.

Da Veiga, A. and J. H. P. Eloff. (2007). "An Information Security Governance Framework," *Information Systems Management* (24) pp. 361-372.

Davis, F. D. (1989). "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *Management Information Systems Quarterly,* Sep.

Dhillon, G. and J. Backhouse. (2001). "Current Directions in IS Security Research: Towards Socio-Organizational Perspectives," *Information Systems Journal* (11)2, pp. 127-153.

Dhillon, G. and S. Chapman. (2007). "To Opt On, or to Opt Out? ThIs Is the Question: A Case Study," *Journal of Information System Security* (2) 2, pp. 46-55.

Dhillon, G. and G. Torkzadeh. (2006). "Value-Focused Assessment of Information System Security in Organizations," *Information Systems Journal* (16), pp. 293-314.

Dinev, T. and P. Hart. (2006). "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17)1, pp. 61-80.

Dinev, T. and Q. Hu. (2007). "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protecting Information Technologies," *Journal of the Association for Information Systems* (8) 7, pp. 386-408.

Duffy, N. M. (1980). "Countdown Services: Fire and its Aftermath in a Computer Bureau," *Information & Management* (3), pp. 103-111.

Egyhazy, C. (1985). "Using Database Machines in Embedded Computer Systems," *Information & Management* (8), pp. 197-203.

Faja, S. and S. Trimi. (2003). "Influence of the Web Vendor's Interventions on Privacy-Related Behaviors in E-Commerce," *Communications of the Association for Information Systems* (17), pp. 2-68.

Fang, X. et al. (2005). "Moderating Effects of Task Type on Wireless Technology Acceptance," *Journal of Management Information Systems* (22)3, pp. 123-157.

Fjermestad, J. et al. (2006). "Moving Towards Mobile Third Generation Telecommunication Standards: The Good and Bad of the 'Anytime/Anywhere' Solutions," *Communications of the Association for Information Systems* (17). Article 3, pp. 2-33.

Frank, J., B. Shamir, and W. Briggs. (1991). "Security-Related Behavior of PC Users in Organizations," *Information & Management* (21), pp. 127-135.

Gal-Or, E. and A. Ghose. (2005). "The Economic Incentives for Sharing Security Information," *Information Systems Research* (16)2, pp. 186-208.

Garfinkel, R., R. Gopal, and S. Thompson. (2007). "Releasing Individually Identifiable Microdata with Privacy Protection against Stochastic Threat: An Application to Health Information," *Information Systems Research* (18)1, pp. 23-41.

Gattiker, U. and H. Kelley. (1999). "Morality and Computers: Attitudes and Differences in Moral Judgments," *Information Systems Research* (10)3, pp. 233-254.

Goodhue, D. L. and D. W. Straub. (1991). "Security Concerns of System Users. A Study of Perceptions of the Adequacy of Security," *Information & Management* (20), pp. 13-27.

Goel, S., A. Baykal, and D. Pon. (2005). "Botnets: The Anatomy of a Case," *Journal of Information System Security* (1)3, pp. 45-60.

Goel, S., D. Pon, and H. Weistroffer. (2006). "Managing Information Security: Demystifying the Audit Process for Security Officers," *Journal of Information System Security* (2)2, pp. 25-44.

Goodman, S. E., and R. Ramer. (2007). "Global Sourcing of IT Sources and Information Security: Prudence before Playing," *Communications of the Association for Information System* (20) article 50, pp. 812-823.

Greenaway, K. E. and Y. E. Chan. (2005). "Theoretical Explanations for Firms' Information Privacy Behaviors," *Journal of the Association for Information Systems* (6) 6, pp. 171-198.

Gupta, A., Y. A. Tung, and J. R. Marsden. (2004). "Digital Signature: Use and Modification to Achieve Success in Next Generational E-business Processes," *Information & Management* (41), pp. 561-575.

Halonen, R. (2006). "Building User Authentication in an -Organizational Information System," *Journal of Information System Security* (2)3, pp. 49-68.

Hammer, C. (1977). "A Forecast of the Future of Computation," *Information & Management* (1), pp. 3-10.

Hammer, C. (1988). "Is Today's Office Receiving Full Value from its Computers?" *Information & Management* (15), pp. 15-23.

Han, S., and S. Cho. (2006). "Evolutionary Neural Networks for Anomaly Detection Based on the Behavior of a Program," *IEEE Transactions on Systems, Man, and Cybernetics –Part B: Cybernetics*. (36)3, pp. 559-570.

Hann, I. et al. (2007). "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach," *Journal of Management Information Systems* (24)2, pp. 13-42.

Harrington, S. (1996). "The Effect of Code of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," *Management Information Systems Quarterly* (20)3, pp. 257-278.

Herzberg, A. (2003). "Payments and Banking with Mobile Personal Devices," *Communications of the ACM* (46)5, pp. 53-58.

Hui, K., H. H. Teo, and S. T. Lee. (2007). "The Value of Privacy Assurance: An Exploratory Field Experiment," *Management Information Systems Quarterly* (31)1, pp. 19-33.

IBM. (2006). IBM Information Security Reference Model, web.esaugumas.lt/storage/conference2006/IBM_ISF%20presentation.%2016-17%20Nov%202006%20(RRT). pps (current as of Nov. 7, 2008).

Im, J. H. and P. D. V. Epps. (1992). "Software Piracy and Software Security Measures in Business Schools," *Information & Management* (23), pp. 193-203.

Ives, B. and V. Krotov. (2006). "Anything You Search Can Be Used against You in a Court of Law: Data Mining in Search Archives," *Communications of the Association for Information Systems* (18). Article 29, pp. 1-28.

Jain, A. K., A. Ross, and S. Pankanti. (2006). "Biometrics: A Tool for Information Security," *IEEE Transactions on Information Forensics and Security* (1)2, pp. 125-143.

JISSEC. (2008). Home Page www.jissec.org (current as of Nov. 7, 2008).

Joseph, G. W. and J. E. Blanton. (1992). "Computer Infectors. Prevention, Detection, and Recovery," *Information & Management* (23), pp. 205-216.

Kim, D. and I. Benbasat. (2003). "A Web Assurance Services Model of Trust for B2C E-commerce," *International Journal of Accounting Information Systems* (4)2, pp. 95-114.

Kim, D. and I. Benbasat. (2006). "The Effects of Trust-Assuring Arguments on Consumer Trust in Internet Stores: Application of Toulmin's Model of Argumentation," *Information Systems Research* (17)3, pp. 286-300.

Kim, H-W., Y. Xu and K. Koh. (2004b). "A Comparison of Online Trust Building Factors between Potential Customers and Repeat Customers," *Journal of the Association for Information Systems* (5) 10, pp. 392-420.

Kim, J. et al. (2002). "Businesses as Buildings: Metrics for the Architectural Quality of Internet Businesses," *Information Systems Research* (13)3, pp. 239-254.

Knapp, K. et al. (2003). "Defense Mechanisms of Biological Cells: A Framework for Network Security Thinking," *Communications of the Association for Information Systems* (12), pp. 701-719.

Koh, C. E. and H. J. Watson. (1998). "Data Management in Executive Information Systems," *Information & Management* (33), pp. 301-312.

Korzyk, A., J. W. Sutherland, and H. Weistroffer. (2006). "A Conceptual Model for Integrative Information Systems Security," *Journal of Information System Security* (2)1, pp. 44-59.

Kotulic, A. G. and J. G. Clark. (2004). "Why There Aren't More Information Security Research Studies," *Information & Management* (41), pp. 597-607.

Lee, S. (2003). "Business Use of Internet-Based Information Systems: The Case of Korea," *European Journal of Information Systems* (12), pp. 168-181.

Lewis, B. R. and T. A. Byrd. (2003). "Development of a Measure for the Information Technology Infrastructure Construct," *European Journal of Information Systems* (12), pp. 93-109.

Lewis B., C. A. Snyder, R. K. Rainer, Jr. (1995). "An Empirical Assessment of the Information Resource Management Construct," *Journal of Management Information Systems* (12)1, pp. 199-223.

Li, Y. and L. Guo. (2007). "An Active Learning Based TCM-KNN Algorithm for Supervised Network Intrusion Detection," *Computers & Security* (26) 7-8, pp. 459-467.

Li, X. and S. Sarkar. (2004). "Privacy Protection in Data Mining: A Perturbation Approach for Categorical Data," *Information Systems Research* (17)3, pp. 254-270.

Lim, N. (2006). "Crime Investigation: A Course in Computer Forensics," *Communications of the Association for Information Systems* (18). Article 10, pp. 2-34.

Littlewood, B. et al. (1993). "Towards Operational Measures of Computer Security," *Journal of Computer Security 2*(3), pp. 211-229.

Loch, K. D., H. C. Carr, and M. E. Warkentin. (1992). "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *Management Information Systems Quarterly* (16)2, pp. 173-186.

Lockman A. and N. Minsky. (1989). "Designing Financial Information Systems for Auditability," *Journal of Management Information Systems* (1)1, pp. 50-62.

Looi, H. C. (2005). "E-Commerce Adoption in Brunei Darussalam: A Quantitative Analysis of Factors Influencing its Adoption," *Communications of the Association for Information Systems* (15), pp. 61-81.

Lucas, H. C. (1985). "Social Security Administration's Progress in Modernizing its Computer Operations," *Information & Management* (9), pp. 283-290.

Ma, Q. and J. M. Pearson. (2005). "ISO 17799: "Best Practices" in Information Security Management?"*Communications of the Association for Information Systems* (15), pp. 577-591.

Malhotra N., S. S. Kim, and J. Agarwal. (2004). "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15)4, pp. 336-355.

McFadzean, E., J. Ezingeard, and D. Birchall. (2006). "Anchoring Information Security Governance Research: Sociological Groundings and Future Directions," *Journal of Information System Security* (2)3, pp. 3-47.

Molla, A., R. Heeks, and I. Balcells. (2006). "Adding Clicks to Bricks: A Case Study of E-Commerce Adoption by a Catalan Small Retailer," *European Journal of Information Systems* (15), pp. 424-438.

Morin, J-H. and M. Pawlak. (2006). "Towards a Global Framework for Corporate and Enterprise Digital Policy Management," *Journal of Information System Security* (2)2, pp. 15-24.

Muntermann, J. and R. Heiko. (2006). “Security Issues and Capabilities of Mobile Brokerage Services and Infrastructures,” *Journal of Information System Security* (2)1, pp. 27-43.

Murray, T. J. (1979). “Cryptographic Transformation of Data Relationships,” *Information & Management* (2), pp. 95-98.

Panko, R. R. (2003). “Slammer: The First Blitz Worm,” *Communications of the Association for Information Systems* (11), pp. 207-218.

Park, I. et al. (2007). “The Effect of Spam and Privacy Concerns on E-Mail Users Behavior,” *Journal of Information System Security* (3)1, pp. 39-62.

Paulson, L. D. (2002). “Wanted: More Network-Security Graduates and Research,” *Computer* (35)2, pp. 22-24.

Pavlou, P. A., H. Liang, and Y. Xue. (2007). “Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective,” *Management Information Systems Quarterly* (31)1, pp. 105-136.

Payne, C. (2002). “On the Security of Open Source Software,” *Information Systems Journal* (12), pp. 61-78.

Payne, J. E. (2004) “Regulation and Information Security: Can Y2K Lessons Help Us?”, *IEEE Security and Privacy Magazine* (2)2, pp. 58-61.

Perlman, R. (2005). “The Ephemerizer: Making Data Disappear,” *Journal of Information System Security* (1)1, pp. 51-68.

Peffers, K. et al. (2007). “A Design Science Research Methodology for Information Systems Research,” *Journal of Management Information Systems* (24)3, pp. 45-77.

Peffers, K. and Y. Tang. (2003). "Identifying and Evaluating the Universe of Outlets for Information Systems Research: Ranking the Journals," *The Journal of Information Technology Theory and Application* (5)1, pp. 63-84.

Peltier, T. (2001). *Information Security Risk Analysis,* Auerbach Publications, Boca Raton, FL.

Post, G. and A. Kagan. (2000). “Management Tradeoffs in Anti-Virus Strategies,” *Information & Management* (37), pp. 13-24.

Ramachandran, S. and G. W. White. (2005). “Methodology to Assess the Impact of Investments in Security Tools and Products,” *Journal of Information System Security* (1)2, pp. 3-25.

Rangnathan, C. and S. Ganapathy. (2002). “Key Dimension of Business-to-Consumer Web Sites,” *Information & Management* (39), pp. 457-465.

Ratnasingham, P. (1998). “Trust in Web-Based Electronic Commerce Security,” *Information Management and Computer Security* (6)4, pp. 162-166.

Ray, I., E. Kim, and D. Massey. (2007). “A Framework to Facilitate Forensic Investigation of Falsely Advertised BGP Routes,” *Journal of Information System Security* (3)2, pp. 32-65.

Reed, A. (2005). “Information Technology and Systems II: Server Administration Networks,” *Communications of the Association for Information Systems* (15), pp. 642-660.

Roberts, C. (2007). “Biometric Attack Vectors and Defences,” *Computers & Security* (26) 1, pp. 14-25.

Rodwell, P. M., S. M. Furnell, and P. L. Reynolds. (2007). “A Non-Intrusive Biometric Authentication Mechanism Utilising Physiological Characteristics of the Human Head,” *Computers & Security* (26) 7-8, pp. 468-478.

Rogers, E. (1995). *Diffusion of Innovation*. New York: Free Press.

Roos, H. (1981). “Confidentiality of Information,” *Information & Management* (4), pp. 17-21.

Ryan, S. D. and B. Bordoloi. (1997) “Evaluating Security Threats in Mainframe and Client/Server Environments,” *Information & Management* (32), pp. 137-146.

Sarathy R. and K. Muralidhar. (2002). “The Security of Confidential Numerical Data in Databases,” *Information Systems Research* (13)4, pp. 389-403.

Schryen, G. (2007). "Do Anti-Spam Measures Effectively Cover the E-Mail Communication Network? A Formal Approach," *Journal of Information System Security* (3)2, pp. 66-90.

Senior Scholars. (2006). Letter to AIS http://home.aisnet.org/associations/7499/files/Senior%20Scholars%20Letter.pdf (Current as of Nov. 7, 2008).

Shadish, W. R., T. D. Cook, and D. T. Campbell. (2002). *Experimental and Quasi-Experimental Designs for Generalized Causal Reference*. Boston-NY: Houghton Mifflin Company.

Shanley, R. and G. Premkumar. (2005). "WIDS: A Wireless Intrusion Detection System for Detecting Man-in-the-Middle Attacks," *Journal of Information System Security* (1)3, pp. 18-44.

Shao, M., J. J. Hwang, and S. Wu. (2005). "A Transactional-Cycle Approach to Evidence Management for Dispute Resolution," *Information & Management* (42), pp. 607-618.

Sharpe, S. (2003). "An ASEAN Way to Security Cooperation in Southeast Asia?" *The Pacific Review* (16)2, pp 231-250.

Shim, J. P., U. Varshney, and S. Dekleva. (2006). "Wireless Evolution 2006: Cellular TV, Wearable Computing, and RFID," *Communications of the Association for Information Systems* (18). Article 24, pp. 1-37.

Shim, J. P. et al. (2007). "Cell Phone TV, Wireless Networks in Disaster Management, Ubiquitous Computing, and Adoption of Future Wireless Applications," *Communications of the Association for Information Systems* (20) Article 29, pp. 1-27.

Siponen, M. T. (2005). "An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice," *European Journal of Information Systems* (14), pp. 303-315.

Siponen, M., R. Baskerville and J. Heikka. (2006). "A Design Theory for Secure Information Systems Design Methods," *Journal of the Association for Information Systems* (7) 11, pp. 725-770.

Siponen, M. and J. Iivari. (2006). "Six Design Theories for IS Security Policies and Guidelines," *Journal of the Association for Information Systems* (7) 7, pp. 445-472.

Slevin, C. (2007). "After Cyber 'Attack', Rockies Are Set to Resume Online Ticket Sales," http://www.redorbit.com/news/technology/1114025/rockies_to_try_online_ticket_sales_again/index.html (current Nov. 7, 2008).

Soliman, K. S. and B. D. Janz. (2004). "An Exploratory Study to Identify the Critical Factors Affecting the Decision to Establish Internet-Based Interorganizational Information Systems," *Information & Management* (41), pp. 697-706.

Spiekermann, S. and H. Ziekow. (2005). "RFID: A Systematic Analysis of Privacy Threat and A Seven-point Plan to Address Them," *Journal of Information System Security* (1)3, pp. 2-18.

Sridhar, V. and D. K. Ahuja. (2007). "Challenges in Managing Information Security in Academic Institutions: Case of MDI India," *Journal of Information System Security* (3) 3, pp. 51-78.

Stafford, T. F. and A. Urbaczewski. (2004). "Spyware: The Ghost in the Machine," *Communications of the Association for Information Systems* (14), pp. 291-306.

Stephens, C. S. and C. A. Snyder. (1991). "An Alternative to Emulation for Micro-Mainframe Data Exchange," *Information & Management* (20), pp. 105-116.

Straub, D. W. (1990a). "Effective IS Security: An Empirical Study," *Information Systems Research* (1)3, pp. 255-276.

Straub, D. W. (1990b). "Key Information Liability Issues Facing Managers: Software Piracy, Proprietary Databases, and Individuals Rights to Privacy," *Management Information Systems Quarterly* (14)2, pp. 143-156.

Straub, D. W. and W. D. Nance. (1990). "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *Management Information Systems Quarterly* (14)1, pp. 45-60.

Straub, D. W. and R. J. Welke. (1998). "Coping with Systems Risk: Security Planning Models for Management Decision Making," *Management Information Systems Quarterly* (22)4, pp. 441-469.

Sumner, M. R. (1986). "An Assessment of Alternative Application Development Approaches," *Information & Management* (10), pp. 197-206.

Sun L., R. P. Srivastava, and T. J. Mock. (2006). "An Information Systems Security Risk Assessment Model Under the Dempster-Shafer Theory of Belief Functions," *Journal of Management Information Systems* (22)4, pp. 109-142.

Swanson, E. B. (1982). "Measuring User Attitudes in MIS Research: A Review," *OMEGA*, (10), pp-157-165.

Tam, K. Y. (1989). "Information Systems for Security Trading," *Information & Management* (16), pp. 105-114.

Tan, M. and T. S. H. Teo. (2000). "Factors Influencing the Adoption of Internet Banking," *Journal of the Association for Information Systems* (1) Article 5, pp. 1-42.

Thuraisingham, B. (1993). "Multilevel Security for Information Retrieval Systems," *Information & Management* (24), pp. 93-103.

Thuraisingham, B. (1995). "Multilevel Security for Information Retrieval Systems II," *Information & Management* (28), pp. 49-61.

Toulmin, S. E. (1958). *The Use of Argument*. Cambridge University Press: Cambridge, UK.

Tryfonas, T. (2007). "On Security Metaphors and How They Shape the Emerging Practice of Secure Information Systems Development," *Journal of Information System Security* (3)3, pp. 21-50.

Turn, R. (1978). "Privacy Protection in Record-Keeping Systems," *Information & Management* (1), pp. 187-197.

Urbach, R. R. and G. A. Kibel. (2004). "Adware/Spyware: An Update Regarding Pending Litigation and Legislation," *Intellectual Property & Technology Law Journal*, (16)7, pp. 12-16.

Van Slyke, C. et al. (2006). "Concern for Information Privacy and Online Consumer Purchasing," *Journal of the Association for Information Systems* (7) 6, pp. 415-444.

Varshney, U. (2003). "Wireless I: Mobile and Wireless Information Systems: Applications, Networks, and Research Problems," *Communications of the Association for Information Systems* (12), pp. 155-166.

Verdon, D. (2006). "Security Policies and the Software Developer," *IEEE Security and Privacy Magazine* (4)4, pp. 42-49.

Verhagen, T., S. Meents, and Y. Tan. (2006), "Perceived Risk and Trust Associated with Purchasing at Electronic Marketplaces," *European Journal of Information Systems* (15), pp. 542-555.

von Solms, B. (2006). "Information Security: The Fourth Wave," Computers & Security (25) 3, pp. 165-168.

von Solms, R. et al. (2005). "A Framework for Information Security Evaluation," *Information & Management* (26), pp. 143-153.

Wang, P. (1994). "Information Systems Management Issues in the Republic of China for the 1990s," *Information & Management* (26), pp. 341-352.

Whitworth, B. and M. Zaic. (2003). "The WOSP Model: Balanced Information System Design and Evaluation," *Communications of the Association for Information Systems* (12), pp. 258-282.

Willison, R. and J. Backhouse. (2006). "Opportunities for Computer Crime: Considering Systems Risk from a Criminological Perspective," *European Journal of Information Systems* (15), pp. 403-414.

Wise Geek, *What Is Information Security?* www.wisegeek.com/what-is-information-security.htm (Current as of Nov.7, 2008)..

Wong, C. K., M. Gouda, and S. S. Lam. (2000). "Secure Group Communications Using Key Graphs," *IEEE/ACM Transactions on Networking (TON)* (8)1, pp. 16-30.

Yang, S. C., S. Chatterjee, and C. C. Chen. (2004). "Wireless Communications: Myths and Reality," *Communications of the Association for Information Systems* (13), pp. 682-696.

Yang, J. and S. S. Huang. (2007). "Mining TCP/IP Packets to Detect Stepping-Stone Intrusion," *Computers & Security* (26) 7-8, pp. 479-484.

Ye, M., G. Premkumar, and D. Zhu. (2007). "An Evaluation of Size-Based Traffic Feature for Intrusion Detection," *Journal of Information System Security* (3)1, pp. 19-38.

Yeh, Q. and A. J. Chang. (2007). "Threats and Countermeasures for Information System Security: A Cross-Industry Study," *Information & Management* (44), pp. 480-491.

Yue W. and M. Cakanyildirim. (2007). "Intrusion Prevention in Information Systems: Reactive and Proactive Responses," *Journal of Management Information Systems* (24)1, pp. 329-353.

Zviran, M. and Z. Erlich. (2006). "Identification and Authentication: Technology and Implementation Issues," *Communications of the Association for Information Systems* (17) Article 4, pp. 2-30.

Zviran M. and W. Haga. (1999). "Password Security: An Empirical Study," *Journal of Management Information Systems* (15)4, pp. 161-185.

ABOUT THE AUTHORS

Humayun Zafar is currently a doctoral candidate in the College of Business at The University of Texas at San Antonio. He holds a Master's of Science degree in Information Technology from the Rochester Institute of Technology, New York. His research interests are economics of IT, security and network design, and wireless communication.

Jan Guynes Clark is a professor of Information Systems at the University of Texas at San Antonio. She received her Ph.D. from the University of North Texas. She is also a Certified Information Systems Security Professional (CISSP). Her research interests include the impact of information technologies on productivity and performance, information security, and IS strategies. Her publications have appeared in leading journals such as *Communications of the AIS, Communications of the ACM, IEEE Transactions on Engineering Management*, and *Information & Management*.

Communications of the Association for Information Systems

ISSN: 1529-3181